

Listing of the Claims:

The following is a complete listing of all the claims in the application, with an indication of the status of each:

1 1 (Currently Amended). ~~An~~ A cryptographic apparatus for computing the sum
 2 of a divisor $D_1 = \text{g.c.d.}((a_1(x)), (y - b_1(x)))$ and a divisor $D_2 = \text{g.c.d.}((a_2(x)),$
 3 $(y - b_2(x)))$ on Jacobian of a hyperelliptic curve $y^2 + y = f(x)$ defined over $\text{GF}(2^n)$,
 4 said apparatus comprising:
 5 a storage for storing $a_1(x)$, $a_2(x)$, $b_1(x)$ and $b_2(x)$; ~~and~~
 6 means for calculating $q(x) = \{s_1(x) (b_1(x) + b_2(x))\} \bmod a_2(x)$ or
 7 $q(x) = \{s_2(x) (b_1(x) + b_2(x))\} \bmod a_1(x)$ by using $s_1(x)$ or $s_2(x)$ in
 8 $s_1(x)a_1(x) + s_2(x)a_2(x) = 1$ in case of $\text{GCD}(a_1(x), a_2(x)) = 1$ where GCD denotes a
 9 greatest common divisor of two polynomials; and
 10 means responsive to said means for calculating for permitting or
 11 denying access to a secure environment.

1 2 (Currently Amended). ~~An~~ A cryptographic apparatus for calculating $a'(x)$
 2 and $b'(x)$ of a reduced divisor $D' = \text{g.c.d.}((a'(x)), (y - b'(x)))$ which is a linearly
 3 equivalent to $D_1 + D_2$ for a divisor $D_1 = \text{g.c.d.}((a_1(x)), (y - b_1(x)))$ and a divisor
 4 $D_2 = \text{g.c.d.}((a_2(x)), (y - b_2(x)))$ on Jacobian of a hyperelliptic curve $y^2 + y = f(x)$
 5 defined over $\text{GF}(2^n)$, said apparatus comprising:
 6 means for calculating $q(x) = s_1(x) (b_1(x) + b_2(x)) \bmod a_2(x)$ by using $s_1(x)$
 7 in $s_1(x)a_1(x) + s_2(x)a_2(x) = 1$ in case of $\text{GCD}(a_1(x), a_2(x)) = 1$ where GCD denotes
 8 a greatest common divisor of two polynomials;
 9 means for calculating $\alpha(x) = Q(q_2(x)a_1(x), a_2(x)) + Q(f(x), a_1(x)a_2(x))$
 10 which is rendered a monic polynomial where $Q(A, B)$ is a quotient of A/B ;
 11 means for calculating $\beta(x) = (q(x)a_1(x) + b_1(x) + 1) \bmod \alpha(x)$;
 12 means for calculating $a'(x) = Q(f(x) + \beta_2(x), \alpha(x))$; ~~and~~
 13 means for calculating $b'(x) = (\beta(x) + 1) \bmod a'(x)$; and

14 means responsive to said last mentioned means for calculating for
 15 permitting or denying access to a secure environment.

1 3 (Currently Amended). ~~An~~ A cryptographic apparatus for computing the sum
 2 of a divisor $D_1 = \text{g.c.d.}((a_1(x)), (y - b_1(x)))$ on Jacobian of a hyperelliptic curve
 3 $y^2 + y = f(x)$ defined over $\text{GF}(2^n)$, said apparatus comprising:

4 a storage for storing $a_1(x)$, and $b_1(x)$; ~~and~~
 5 means for calculating $q(x) = Q(b_1^2(x) + f(x) \bmod a_1^2(x), a_1(x))$ where
 6 $Q(A, B)$ is a quotient of A/B ; and

7 means responsive to said means for calculating for permitting or
 8 denying access to a secure environment.

1 4 (Currently Amended). ~~An~~ A cryptographic apparatus for calculating $a'(x)$
 2 and $b'(x)$ of a reduced divisor $D' = \text{g.c.d.}((a'(x)), (y - b'(x)))$ which is a linearly
 3 equivalent to $D_1 + D_1$ for a divisor $D_1 = \text{g.c.d.}((a_1(x)), (y - b_1(x)))$ on Jacobian of a
 4 hyperelliptic curve $y^2 + y = f(x)$ defined over $\text{GF}(2^n)$, said apparatus comprising:

5 means for calculating $q(x) = Q(b_1^2(x) + f(x) \bmod a_1^2(x), a_1(x))$ where
 6 $Q(A, B)$ is a quotient of A/B ;

7 means for calculating $\alpha(x) = q_2(x) + Q(f(x), a_1^2(x))$ which is rendered a
 8 monic polynomial;

9 means for calculating $\beta(x) = b_1^2(x) + f(x) \bmod a_1^2(x) + 1 \bmod \alpha(x)$;

10 means for calculating $a'(x) = Q(f(x) + \beta_2(x), \alpha(x))$; ~~and~~

11 means for calculating $b'(x) = (\beta(x) + 1 \bmod a'(x))$; and

12 means responsive to said last mentioned means for calculating for
 13 permitting or denying access to a secure environment.

1 5 (Currently Amended). A computer implemented cryptographic method for
 2 calculating $a'(x)$ and $b'(x)$ of a reduced divisor $D' = \text{g.c.d.}((a'(x)), (y - b'(x)))$
 3 which is a linearly equivalent to $D_1 + D_2$ for a divisor $D_1 = \text{g.c.d.}((a_1(x)),$

4 $(y - b_1(x))$ and a divisor $D_2 = \text{g.c.d.}((a_2(x)), y - b_2(x))$ on Jacobian of a
 5 hyperelliptic curve $y^2 + y = f(x)$ defined over $\text{GF}(2^n)$, said method comprising the
 6 steps of:
 7 calculating and storing in a storage $q(x) = \{s_1(x) (b_1(x) + b_2(x))\}$
 8 mod $a_2(x)$ by using $s_1(x)$ in $s_1(x)a_1(x) + s_2(x)a_2(x) = 1$ in case of
 9 $\text{GCD}(a_1(x), a_2(x)) = 1$ where GCD denotes a greatest common divisor of two
 10 polynomials;
 11 calculating and storing in a storage $\alpha(x) = Q(q^2(x)a_1(x), a_2(x)) + Q(f(x),$
 12 $a_1(x)a_2(x))$ which is rendered a monic polynomial where $Q(A,B)$ is a quotient
 13 of A/B ;
 14 calculating and storing in a storage $\beta(x) = (q(x)a_1(x) + b_1(x) + 1) \bmod$
 15 $\alpha(x)$;
 16 calculating and storing in a storage $a'(x) = Q(f(x) + \beta^2(x), \alpha(x))$; and
 17 calculating and storing in a storage $b'(x) = (\beta(x) + 1) \bmod a'(x)$; and
 18 permitting or denying access to a secure environment depending on an
 19 outcome of said calculating steps.

1 6 (Currently Amended). A computer implemented cryptographic method for
 2 calculating $a'(x)$ and $b'(x)$ of a reduced divisor $D' = \text{g.c.d.}((a'(x)), y - b'(x))$
 3 which is a linearly equivalent to $D_1 + D_1$ for a divisor $D + D_1 = \text{g.c.d.}((a_1(x)),$
 4 $(y - b_1(x)))$ on Jacobian of a hyperelliptic curve $y^2 + y = f(x)$ defined over $\text{GF}(2^n)$,
 5 said method comprising the steps of:
 6 calculating and storing in a storage $q(x) = Q(b_1^2(x) + f(x) \bmod a_1^2(x), a_1)$
 7 where $Q(A,B)$ is a quotient of A/B ;
 8 calculating and storing in a storage $\alpha(x) = q^2(x) + Q(f(x), a_1^2(x))$ which is
 9 rendered a monic polynomial;
 10 calculating and storing in a storage $\beta(x) = (b_1^2(x) + f(x) \bmod a_1^2(x) + 1)$
 11 mod $\alpha(x)$;
 12 calculating and storing in a storage $a'(x) = Q(f(x) + \beta^2(x), \alpha(x))$; and

13 calculating and storing in a storage $b'(x) = (\beta(x) + 1) \bmod a'(x)$; and
 14 permitting or denying access to a secure environment depending on an
 15 outcome of said calculating steps.

1 7 (Currently Amended). A computer implemented cryptographic method for
 2 computing the sum of a divisor $D_1 = \text{g.c.d.}((a_1(x)), (y - b_1(x)))$ and a divisor
 3 $D_2 = \text{g.c.d.}((a_2(x)), (y - b_2(x)))$ on Jacobian of a hyperelliptic curve $y^2 + y = f(x)$
 4 defined over $\text{GF}(2^n)$, said method comprising the steps of:
 5 storing $a_1(x)$, $a_2(x)$, $b_1(x)$ and $b_2(x)$; and
 6 calculating and storing in a storage $q(x) = \{s_1(x) (b_1(x) + b_2(x))\} \bmod$
 7 $a_2(x)$ or $q(x) = \{s_2(x) (b_1(x) + b_2(x))\} \bmod a_1(x)$ by using $s_1(x)$ or $s_2(x)$ in
 8 $s_1(x)a_1(x) + s_2(x)a_2(x) = 1$ in case of $\text{GCD}(a_1(x), a_2(x)) = 1$; and
 9 permitting or denying access to a secure environment depending on an
 10 outcome of said calculating step.

1 8 (Currently Amended). A computer implemented cryptographic method for
 2 computing the sum of a divisor $D_1 = \text{g.c.d.}((a_1(x)), (y - b_1(x)))$ on Jacobian of a
 3 hyperelliptic curve $y^2 + y = f(x)$ defined over $\text{GF}(2^n)$, said method comprising the
 4 steps of:
 5 storing $a_1(x)$, and $b_1(x)$; and
 6 calculating and storing in a storage $q(x) = Q(b_1^2(x) + f(x) \bmod a_1^2(x),$
 7 $a_1(x))$ where $Q(A, B)$ is a quotient of A/B ; and
 8 permitting or denying access to a secure environment depending on an
 9 outcome of said calculating step.